CASE STUDY

Fujitsu Technology and Business of America Prevents Prospective Employee Data Leakage with FinalCode

CHALLENGE

Fujitsu Technology and Business of America needed a file-centric information rights management (IRM) solution that was easy to implement and could be scaled throughout the division immediately.

SOLUTION

FinalCode's ability to track files in and outside of the company—as well as its stability, scalability and flexibility— were ideal for the size and scope of Fujitsu Technology and Business of America's organization.

Technology businesses are consistently poised for rapid growth and often need hiring support from external recruiting and human resources firms to keep up. Paired together, these companies work in a highly connected world where sharing files and collaborating online is the norm.

The recruiting and job application process generates a significant amount of sensitive information, mainly belonging to applicants. Resumes not only include names, address and contact information but entire work histories and, potentially, salary information. Plus, job descriptions contain insights into a business's current needs and vacancies, which, in the wrong hands, could be used to gain competitor intelligence or craft convincing spear phishing attacks. All of this data needs to be protected from hackers, malicious users and human error alike.

Fujitsu Technology and Business of America (FTBA) provides technology and business support services to Fujitsu Limited and 17 Fujitsu-affiliated companies in the U.S. These services include support in IT Subaru telescope operations, R&D engineering, marketing, patent filing, procurement operations, accounting, tax, facilities, risk management, employee benefit programs, HR & HR assignees, and more.

> *"The return on investment, knowing that we are treating our future employees' information with care and starting our relationship on a trustworthy note, is invaluable."*
>
> *– Masaki Maruyama, Manager, Research and Engineering, International Procurement Operations at FTBA*

With 100,000 employees and an expanding business touching so many sectors, like many tech firms, FTBA works with recruiting organizations to help in hiring the best and brightest to join its team. As prospective employees navigate the hiring process, FTBA has made building and keeping trust with these applicants a top priority. So it quickly became evident that the security of the data it houses needed to be of the utmost importance.

Fujitsu Technology and Business of America Prevents Prospective Employee Data Leakage with FinalCode

FTBA realized that once the information from the recruiting company was in its hands, it became its responsibility to keep it safe and secure—and reputational and financial damage caused by data leakage was simply not an option.

Without proper file protection and auditing controls, personal identifiable information (PII) found in recruiting files remained open to unauthorized access and misuse. The firm needed a file-centric information rights management (IRM) solution that was easy to implement and could be scaled throughout the division immediately.

FTBA's skilled IT team evaluated FinalCode and its competitor Vera, which was deemed unstable, and ultimately selected FinalCode's persistent file security platform. FinalCode's ability to track files in and outside of the company—as well as its stability, scalability and flexibility— were ideal for the size and scope of FTBA's organization.

> *FinalCode implemented the solution as a software-as-a-service (SaaS), enabling FTBA to cost effectively deploy the comprehensive solution in a short, manageable timeframe.*

Information meant only for companies' internal use, such as resumes and job descriptions, can sometimes end up in the wrong hands. This is no longer an issue for FTBA. If any collaborator inappropriately or inadvertently shares a sensitive file with an unauthorized user, mishandles it accidentally or has it stolen, FinalCode can deny access and log the attempt.

FinalCode also enables very granular controls for FTBA, over who can access files, under what conditions and what they can do with them. Users can easily apply required controls on file viewing, editing, saving, printing, and watermarking. More so, the file owner can change the file security policy dynamically and even remotely delete files after they have been shared—a major selling point for FTBA. These security policy controls are enforced wherever the file goes and every time the sensitive file is opened.

FinalCode implemented the solution as a software-as-a-service (SaaS), enabling FTBA to cost effectively deploy the comprehensive solution in a short, manageable timeframe. The FinalCode Server, available as a service or on-premise virtual appliance, holds encryption keys and entitlement restrictions, authenticates users against a directory, conveys usage controls to the FinalCode Client, and tracks usage for comprehensive file activity auditing. The free client can be quickly installed as needed, by department, project or enterprise-wide, and importantly, can be easily used by job candidates and external partners if needed.

"Humans can make mistakes. We could have the perfect firewall and external security measures to prevent hacking. However, those tools do not account for human error—for example, an employee emailing a resume to the wrong person. FinalCode's persistent file security offers that extra layer of protection," said Masaki Maruyama, Manager, Research and Engineering, International Procurement Operations at FTBA. "The return on investment, knowing that we are treating our future employees' information with care and starting our relationship on a trustworthy note, is invaluable."

About FinalCode
FinalCode delivers a file security platform that allows any business to persistently protect sensitive files wherever they go inside and outside of the organization. Available as a SaaS or virtual appliance, FinalCode makes securing file collaboration easy and cost-effective and in a way that works with popular applications, platforms and devices while preserving user experience and workflow. The solution applies strong encryption and granular usage control on demand or by corporate policy with the ability to remotely delete files. The company's patented CryptoEase™ technology streamlines onboarding, encryption and administration, making deployment rapid and scalable. Headquartered in San Jose, California, FinalCode offers its solutions through its global network of authorized partners. Learn more at http://www.finalcode.com.